The System Life Cycle and Integrated System Health Engineering and Management

Charles D. Mott
University of North Dakota, Department of Space Studies, Grand Forks, ND 58202
cdmott@space.edu
701-740-2582

University of North Dakota

System Health Management

- Eliminate Failures by
  - Designing and building the system in a manner that reduces the number of failure modes to a minimum
  - Fully testing, verifying, and validating the system to uncover faults in workmanship, materials, or performance
  - Integrating fault tolerance into the system to allow for the detection, isolation, and recovery from failures
  - Identifying and documenting failure causes and using this information to improve future designs

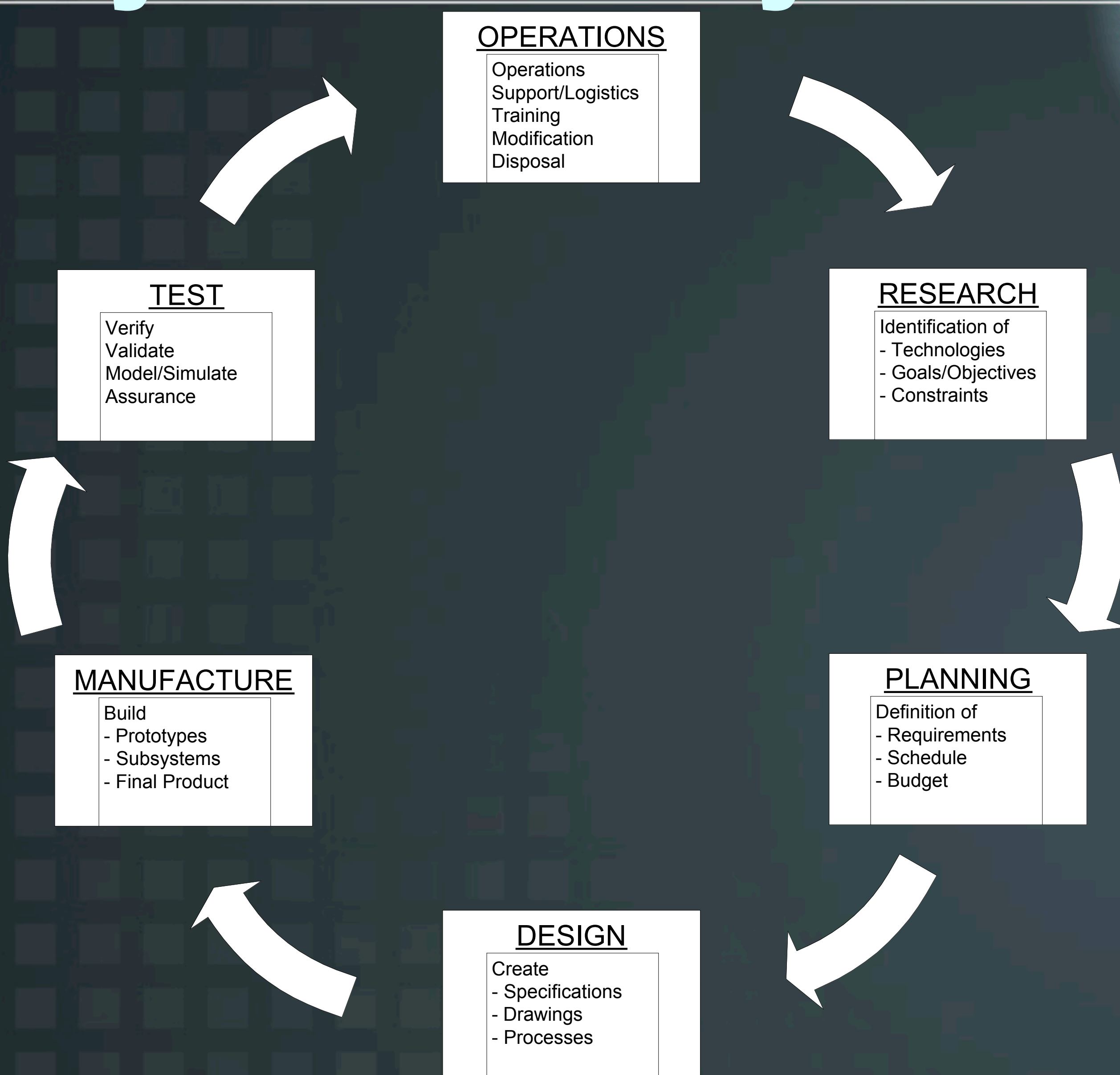
Campbell *et al.*, 1992

System Health Management

ISH(E)M

- Integrated
  - Combination of multiple disciplines
- System
  - Complex, Interdependent, High-Tech
- Health
  - Dependability, Operates as intended
- Engineering
  - Designed into the system
- Management
  - Human-machine interaction throughout the life cycle

The System Life Cycle



System Health Management

Observations

- Multi-disciplinary
  - Engineering, Management, Social
- Communication
- Cradle-to-Grave Process
- ISHEM is not a SHM subsystem
  - Design methodology
  - Eliminate failure potential across system life cycle phases
    - Early design decisions and their effect on operations
    - Built-in failure modes due to system level interactions
    - Testing that is isolated by mission phases/actions

Objectives

- Organize ISHEM Methods
- Show Interconnected Nature of SLC
- Find Opportunities for
  - Better Data Sharing
  - Increased Efficiencies
  - Reduced Costs
  - Improved Dependability

Framework

Theory or Discipline	System Life-Cycle Phase					
	Research	Planning	Design	Manufacture	Testing	Operations
Configuration Management			H	H	M	M
Data Analysis and Mining	H					M
Design Methods and Fault Management			H			M
Diagnostics			M		H	H
Economics of System Integration		M		H		
Failure Assessment	H		M			
Failure Statistics, Data Collection and Dissemination	H	M				M
Fault Modes & Effects Analysis		M	H		M	
Fault Tolerant Computing and Architectures	H		M			M
High Reliability Organizations	M	M				H
Human Factors		M	M	M	M	H
Interface Control		M	H	M		
Knowledge Management		H	M	M	M	M
Maintainability Theory and Practice		M				H
Management Structure	M	M	M	M	H	H
Physics of Failure	H				M	
Probabilistic Risk Assessment	H	M				
Prognostics			M		H	H
Quality Assurance			M	H		M
Reliability Theory and Practice	H	M		M	M	
Risk Management		H			M	M
Safety and Hazard Analysis		H			M	M
Simulation/Modeling		M	H		H	M
Time to Criticality Analysis		M	H			
Verification and Validation		M	M		H	M

H = high influence M = moderate influence blank = low influence

Research

- Identify Technologies and Methods
- Basic and Applied Research
- Technology Maturation
- Reduce Uncertainty
- Need to Spend More Effort Developing Needs, Goals, Objectives, and Scope
- Document and Utilize Results in Subsequent Phases
- Overcome Cultural Influence

Planning

- Define System Requirements
- Set Budget
- Set Schedule
- Form Project Team
- Place More Emphasis on Writing Good Requirements
- Develop Realistic Costs / Schedule Estimates
- Base Plans on Operation Concepts

Design

- Functional Breakdown
- Create Specifications
  - Materials
  - Layout (Drawings)
  - Mass Budget
  - Power Budget

- Increase Awareness of the Effects of Interfaces and the Interactions Between Subsystems
- Develop Methods of Using Models / Simulations to Increase Dependability During Operations
- Design For
  - Performance (Status Quo)
  - Dependability
  - Usability
  - Survivability
  - Supportability
  - Maintainability
  - Affordability (Up-Front vs. Operations)

Manufacture

- Create
  - Prototypes
  - Assemblies
  - Subsystems
- Final Integration

- Evaluate the Need for Concurrency
  - Leftover from Cold War
  - Creates Additional Interfaces
  - Need for Greater Communication / Coordination Among Multiple Organizations
- Monitor Quality Assurance Programs

Testing

- Verification and Validation
- Simulations

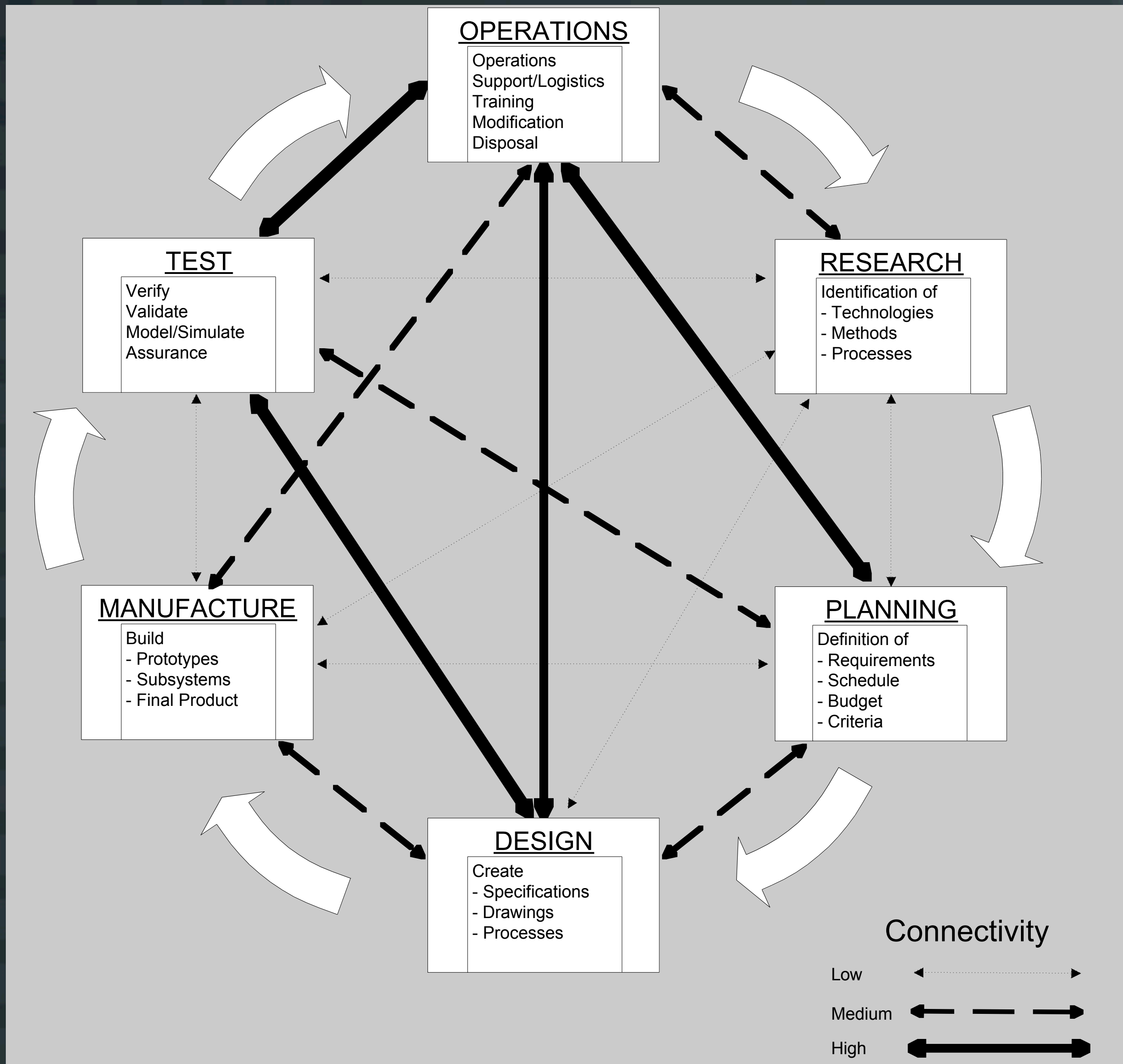
- Need for Independent Verification and Validation Methods
- Testing Takes Place in All Phases
- Testing Can be Used to Evaluate Initial Selections

Operations

- Operations
- Support
- Training
- Maintenance
- Disposal

- Operations Costs Can be Greatly Affected by Design Considerations
- Operators Should have Greater Input in Early Design Decisions
- Collection of Operational Data on Successes and Failures is Essential to Improve Future Systems
- Operators Need Access to Design Information when Off-Nominal Conditions Occur

The System Life Cycle



System Approach

. . . although the methodology is most easily described as a sequence of phases, it is not necessary to move from phase to phase: what is important is the content of the individual phases and the relationships between them. With that pattern established, the good systems thinker will use them in any order, will iterate frequently, and may well work simultaneously on more than one phase. This ‘out of sequence’ usage is particularly important in tackling broad problems which are not owned within a single organization.

(Peter Checkland, 1981, *Systems Thinking, System Practice,* New York, Wiley & Sons, pg. 17).

Further Research

- How to Include ISHEM in System Engineering Education/Application
- Include Additional Methods/Techniques